Statement of

Dr. John A. Gauss

Assistant Secretary for Information and Technology

Department of Veterans Affairs

Before the

Subcommittee on Oversight and Investigations

Committee on Veterans' Affairs

U. S. House of Representatives

September 26, 2002

Good morning, Mr. Chairman and members of the Subcommittee. On behalf of the Secretary of Veterans Affairs, I am pleased to have this opportunity to come here today and update you on the progress the Department has made in strengthening our Information Technology program, and specifically address issues relating to:

- VA's Enterprise Architecture;
- VA's Cyber Security program;
- The recent realignment of the Department's IT structure; and,
- Issues raised at the March 13, 2002, IT hearing.

On March 13, 2002, I appeared before this Subcommittee and gave you my personal commitment to reform the way VA uses information technology. I committed to:

- Publishing an approved Enterprise Architecture Implementation Plan by no later than 30 April 2002;
- Ensuring that networks and systems we depend upon are made secure and available;
- Personally overseeing VETSNET to ensure its progress meets the projected time of being ready to deploy by April 2004 or recommending to the Secretary that the effort be terminated; and,
- Conducting a deployment review for the Government Computer Based Patient Records (GCPR) program to ensure a quality product can be effectively deployed.

With respect to Enterprise Architecture (EA), the Department published a detailed Implementation Plan on April 22, 2002, and undertook the development of the initial version of the One-VA Enterprise Architecture. As a result of successfully executing the Implementation Plan, the Secretary approved version 1.0 of the One-VA Enterprise Architecture on September 5, 2002. It provides a clear pathway for the transformation of both business processes and Information Technology to support these business processes across the Department.

Version 1.0 of the One-VA EA establishes ten Enterprise Business Functions (EBFs) and seven Key Enabling Functions (KEFs) that provide a top-level view of the Department's operations from a top-down, business-focused perspective. These EBFs and KEFs are as follows:

Enterprise Business Functions

- Compensation
- Pension
- Vocational Rehabilitation & Employment
- Education
- Insurance
- Home Loan Guaranty
- Memorials & Burial
- Medical Care
- Medical Education
- Medical Research

Key Enabling Functions

- Finance and Accounting
- Acquisition & Materiel Management
- Information Technology
    - Telecommunications
    - Cyber Security
    - Data Center COOP
- Human Resources
- Training & Education
- Registration & Eligibility
- Contact Management

Several of these EBFs and KEFs were identified as significant opportunities for functional consolidation and integration to collapse redundant processes and the duplicative IT systems that support them and implement a transformational, One-VA approach to dealing with veterans. These include Registration and Eligibility that will collapse eight separate business processes into one, and Contact Management that will provide a single multi-media face for the Department in interacting with veterans and collapse five redundant business processes into one. They also include the Health Data Repository (HDR), which will set the foundation for transforming VA medical care from "facility centric" to "patient centric" health care.

From the perspective of Information Technology Infrastructure to support the EBFs and KEFs, the One-VA EA describes the distributed computing model and technical architecture for the future. The top layer of the model represents how data and applications will interrelate in the future. It is where VA will implement the functional consolidation described previously in One-VA Registration and Eligibility, Contact Management and Health Data Repository.

The layer below the data/applications layer represents corporate and regional computing services to store the data and run the applications. VA will consolidate corporate data center operations to establish a single corporate data center distributed across three widely dispersed locations. These three locations will operate under a single management structure and be linked with one another with high performance data telecommunications so they appear logically as a single entity. They will provide Continuity of Operations (COOP) support for electronic data vaulting, applications restart and business process restart in the event of a disaster. Regional data centers will also support the EA's distributed computing model in transitioning VA from a "facility centric" computing environment to a "network centric" computing environment to support mid-tier and office automation capability. In the end state, this effort will remove many servers from end user facilities and replace them in regional locations with COOP capability designed in. This will lead to significant reduction in hardware costs for the future, reduce the skills required at the local level to operate and maintain the capability, and significantly enhance our cyber security posture.

The next lower layer in the distributed computing model is for cyber security functions to protect the computing infrastructure against cyber attack. The bottom layer is a One-VA national data network. We are well on our way to implementing the One-VA data network and the Cyber Security functions to protect our computing environment.

Specific progress since the last hearing follows:

- The Department of Veterans Affairs “One-VA Enterprise Architecture Implementation Plan: FY 2002” was approved on April 22, 2002;
- The Secretary approved the Department of Veterans Affairs “One-VA Enterprise Architecture Version 1.0” on September 5, 2002;
- Staffing has been approved for the Enterprise Architecture Office and recruitment for these positions is underway; and,
- The position for an SES level Chief Architect has been approved and recruitment for this position is underway.

As I discussed in my March 13, 2002, testimony before this Subcommittee, our current data network is overly complex, too expensive for the performance it provides, and does not have an enterprise-wide network management capability. This complexity and lack of network management capability seriously impede our ability to properly secure and assure network services. To correct these deficiencies, we have embarked on a project to re-architect our data network and change the network from a circuit-based network to a performance-based network. The VA Strategic Management Council reviewed and the Deputy Secretary has approved executing the first phase of this project. The detailed Business Case Analysis, Cost Benefit Analysis, Return on Investment Analysis, and Analysis of Alternatives were completed. These analyses showed that converting our data network from a circuit-based network to a performance-based network will:

- Simplify the complexity;
- Substantially improve performance in support of our EA efforts;
- Establish a network management capability;
- Significantly improve the security and assurance of service; and,

- Provide savings to our current data network budget.

Phase I of this project involved the transfer of responsibility for the Operations & Maintenance of the data network backbone to SPRINT, one of the FTS2001 telecommunications providers. Phase I also involves standardizing equipment and software configurations across the data network backbone. Phase I will be complete by the end of this month. Since transferring this responsibility to SPRINT in April 2002, we have significantly improved network backbone effective throughput and reliability. The next phase of this project will optimize the network's backbone performance. We will start this optimization next week.

With respect to cyber security, the Department has made significant progress in correcting the deficiencies identified by our Office of Inspector General (OIG) and the General Accounting Office (GAO). This year, the Department fielded one of the largest anti-virus capabilities in the world, as well as awarded a multi-year contract to significantly enhance the VA's central incident response capability.

VA recently established a global anti-virus capability to protect the over 140,000 desktops connected to VA's Intranet from malicious attack. To date, over two million viruses have been successfully detected and eradicated. This effort is continuing through providing additional role-based training to ensure that IT personnel are knowledgeable about associated equipment operating characteristics and maintenance requirements; hardening servers consistent with optimized site configuration; and, establishing an Anti-virus analytical and warning capability. This capability uses an automated tool that, within minutes of a virus attack on a VA computer, can identify the incident by virus type, version, and specific location of the equipment under attack. When a virus attack is detected, a warning is concurrently sent to the VA Central Incident Response Capability (VA-CIRC), which will issue a Department-wide anti-virus alert.

After a rigorous several-month effort, a contract to significantly upgrade the capabilities of our VA-CIRC was awarded during July. The contract winner, which is now known as the VA Security Team, or VAST, is a consortium of five small businesses, led by SecureInfo Corporation. There are three large companies that are under subcontract to provide specific niche services when required. In the near future, this enhanced VA-CIRC capability will become the nucleus of all VA information and Internet security operations nationwide, providing such global services as firewall management and Intrusion Detection System (IDS) monitoring.

The VA anti-virus program will be integrated with the enhanced VA-CIRC capability, and associated vendor releases, security bulletins, security alerts, and patch distribution will be tailored for the specific existing configuration of each VA facility. This will afford immediate management attention to priority issues, instead of the current situation wherein IT staff and security personnel must evaluate all alerts for relevancy to their operations. The VA-CIRC has begun testing the effectiveness of facility-implemented security controls through vulnerability and penetration scanning tests. This exemplifies the total “cradle to grave” solution that is required to effectively address emerging threats to VA’s networks on an expedient basis.

In addition to the anti-virus and VA-CIRC efforts, the Department is continuing to deploy other specifically focused initiatives developed during the past year to correct IT security weaknesses identified in our annual Government Information Security Act (GISRA) self-assessment survey process. These programs include our Enterprise Cyber Security Infrastructure Project (ECSIP), the Information Security Technology Certification and Accreditation Program (ITSCAP), and our newly-established Cyber Security Professionalization and Compliance Programs.

The ECSIP program, which was discussed during the March testimony, will implement Department-wide intrusion detection, and firewall capability with a concurrent significant reduction in external network gateways. This project, which was approved by the Department’s Strategic Management Council in February 2002, coincides with VA’s telecommunications network modernization. As part of the project, we plan to systematically collapse the over 200 existing external network gateways in VA into a more manageable number and efficient structure. Concurrent with this effort, Department-wide IDS capability will be incrementally deployed on a strategic basis to provide significantly increased security protections for these gateways. The IDS effort will include real-time analytical incident support, as well as information sharing capabilities regarding emerging threats and vulnerabilities. Design and implementation efforts for this standardized architecture and configuration are underway and we anticipate deploying the initial capability during the first quarter of calendar year 2003.

ITSCAP, the Department’s comprehensive Certification and Accreditation (C&A) process, will ensure that IT systems undergo a rigorous security review prior to being authorized to process sensitive data. An accompanying ITSCAP Handbook of procedures and guidance, which articulates the specific actions, document reviews, and required analyses associated with the C&A process, places increased emphasis on the system and/or major application security plan, and on physical security, through a “site-specific” accreditation process.

The Department’s newly-established Cyber Security Professionalization Program (CSPP) will provide general and role-specific training, career progression, and incentives targeted toward development of a highly skilled and motivated cadre of VA cyber security practitioners. In addition to existing VA Information Security Officer (ISO) training modules, other elements being considered for inclusion in the CSPP include: training and testing specific to Federal and VA guidelines for IT security; training and testing specific to topical areas included in industry-recognized professional certifications; and, career development opportunities through formalized position descriptions which delineate a range of ISO skill levels to support Department-wide career paths.

Additionally, the CSPP will provide professional certifications for those VA employees who meet stringent qualifications through combinations of training, testing, and experience. The Department will maintain pertinent information on individual cyber security practitioner certification status, evaluate the proficiency of current credential holders on a periodic basis, and take appropriate action to suspend and/or revoke cyber security practitioner credentials for any individual who fails to adhere to established standards.

A Compliance Program will provide independent verification of adherence to Department security policies and procedures through continual assessment of documentation archived in the Department's GISRA database, and subsequent periodic site visits to verify and test related IT security control implementation. The results of these reviews will be provided to facility directors and Department senior management personnel to ensure that personnel initiate prompt action to correct identified deficiencies. Additionally, the reviews will be used to develop a process for routinely identifying trends and vulnerabilities, and applying appropriate countermeasures to improve security.

The Secretary approved the establishment of the professionalization and compliance programs to respond to concerns expressed by the OIG regarding the unevenness of reporting in the Department's GISRA database, as well as to preclude instances such as the one that occurred in the Indianapolis Medical Center this past spring.

In summary of our cyber security efforts, we are building a strong foundation for our IT program, but much remains to be done.

In a memorandum signed by the Secretary on August 6, 2002, he directed that all IT personnel and resources be centralized under the Office of Information and Technology. The first action I took was to assign the Administration Chief Information Officers to be Department Deputy CIOs for Health, Benefits and Memorial Affairs. Further, the senior IT manager in each Central Office staff office that operates and maintains IT networks and equipment now report directly to me.

Initially, I have focused on establishing a clear, unambiguous reporting chain for the Department's cyber security efforts. We have developed an organizational structure that combines the cyber security staff elements of the Administrations with the Central Office's Cyber Security staff, thereby creating a single integrated cyber security program office for the Department. Further, field Information Security Officers (ISOs) at the VHA VISN level and at the VBA Network Service Center (NSC) level will become direct reports to the Office of Cyber Security early next fiscal year. Within each hospital, regional office and at each cemetery, the ISOs will report directly to their respective facility director rather than the inconsistent manner of reporting in the past. The VISN and NSC ISOs will provide functional cyber security direction to the facility ISOs, and conduct periodic inspections of the Cyber Security activities at each facility under their purview. The facility ISOs will be required to submit weekly reports as to each facility's cyber security health and welfare.

With respect to financial accountability, I am requiring financial execution plans, or spend plans, to be submitted to me for approval prior to the start of each fiscal year. These spend plans define what work will be done, who will do the work, how much will be spent and when it will be spent. I am pleased to report that I have received these spend plans for fiscal year 2003 that cover the planned IT expenditures for each administration. I am also pleased to report that the quality of these spend plans far exceeded my expectations for the initial submission. These spend plans will give my office the opportunity to drill down into each planned expenditure to ensure that they will not only satisfy mission need but will also comply with the recently published version 1.0 of the Enterprise Architecture. Although the quality of the initial spend plan submissions far exceeded my expectations, some spend plans require additional work to provide a greater degree of detail. This work will be completed prior to the end of the calendar year.

I have convened a group of senior leaders from the Department to develop a detailed reorganization package to submit to the Secretary no later than November 1, 2002. This reorganization package will provide the detail associated with the specific centralization of authority from an organizational perspective, and provide detailed staffing descriptions for each of the organizational elements. In addition to the reorganization of the cyber security functions discussed above, the group will help me determine how best to consolidate duplicative staff functions, centralize the reporting responsibilities of our data centers and our IT system development activities, and consolidate the Central Office IT networks and computing facilities.

Concerning VETSNET, as I committed to you at the last hearing, I have been personally overseeing the progress of this effort along with the Under Secretary for Benefits. On June 17, 2002, the Secretary received a comprehensive review of our plans to correct the Department's outstanding IT deficiencies as reported by the General Accounting Office. This review included a detailed discussion on VETSNET. Required actions to be completed by the end of September include:

- Selecting a full time VETSNET project manager to have the responsibility and accountability for cost, schedule and performance for the completion of this effort;
- Contracting for an independent test activity to ensure that the system will meet all of its performance requirements;
- Validating that all of the performance requirements are correct (except for reports that are d ue by the end of the calendar year); and,
- Conducting a review of the readiness of the program to meet the April 2004 date that was promised at the last hearing.

I am pleased to report that these actions are complete and, in conjunction with the Under Secretary for Benefits, we have recommended to the Secretary that we continue the VETSNET effort in FY2003.

With respect to the Government Computer Based Patient Records (GCPR) program, we have re-baselined and re-scoped the program to address issues identified in a 2001 GAO report. We have renamed GCPR to be the Federal Health Information Exchange (FHIE) program. The re-baselined FHIE program uses an existing VA application called the Computerized Patient Record System (CPRS) as a fundamental building block. CPRS enables a clinician to access clinical data from any VA health facility. FHIE is a database that receives DoD clinical data (an exception being physician notes which are not electronically available from DoD at this time). CPRS is the application that enables VA to import clinical data from the FHIE database in addition to clinical data available within VA.

On April 26, 2002, I chaired a review of the FHIE test results to determine whether or not the first phase of FHIE is ready for deployment. Based on the results of this review, I determined that FHIE was ready to deploy on May 27, 2002. Deployment of this first phase of FHIE was completed in July 17, 2002. Future investment in FHIE will enhance functionality based on clinician feedback once operational.

On May 3, 2002, the Deputy Secretary, Department of Veterans Affairs, and the Under Secretary (Personnel and Readiness), Department of Defense signed a Memorandum of Agreement (MOA) for the Federal Health Information Exchange Governance and Management. This MOA:

- Replaces original GCPR documents signed in 1998;
- Renames GCPR to Federal Health Information Exchange (FHIE);
- Designates VA as the lead agency for FHIE (formerly GCPR);
- Revises goals and objectives to be aligned with the current strategy and direction of the project; and,
- Commits executive level support necessary to adequately manage the project.

I believe that the issues addressed in the April 2001 GAO report on GCPR have been addressed by the above actions.

I hope I have provided some insight as to the progress that has been made since the March 13, 2002, hearing. I believe these efforts demonstrate our very strong commitment, at all levels, to building an effective information technology program for the long-term. With your assistance, we will be able to continue on this path forward to ensure our continued ability to service the health and benefit requirements of our veteran population and their dependents.

Thank you for this opportunity to discuss these very important IT issues. I will be happy to answer your questions.